REMARKS

Claims 1-22 are pending in the application. Claim 16 has been amended. Reconsideration of this application is respectfully requested.

Claim 16 has been amended to clarify that the devices recited in claim 16 are first and second devices.

The Office Action rejects claims 1, 2, 5, 9, 10, 12, 16-19 and 21 under 35 U.S.C. 102(b) as anticipated by U.S. Patent No. 6,735,702 to Yavatkar et al., hereafter Yavatkar.

This rejection is erroneous for the reason that Yavatkar lacks one or more steps or elements recited in these claims as discussed below.

With respect to claim 1, the Examiner, citing col. 13, lines 30-43, for support, contends that Yavatkar discloses "operating a traceback program on at least one path to receive two input parameters, (a) an IP address (v) of the victim machine and (b) an IP address (r) of a router that is immediately upstream of the victim machine", as recited in claim 1. However, the cited text does not disclose this recitation. Rather, the cited text merely teaches a system that can be used to trace attacks, but that is all that it says. The cited text does not disclose the particulars of parts (a) and (b) of the claim 1 recitation.

The Examiner, citing col. 16, line 66 – col. 17, line 31, for support, contends that Yavatkar discloses "determining a set of routers that are neighbors (n) of r", as recited in claim 1. However, the cited text clearly does not disclose this recitation of claim 1. The cited text does not teach to determine routers that are neighbors of an IP address r of a router that is immediately upstream of the victim. The cited text merely says "the bloodhound agent first moves to a device (typically a router) closest in the network topology to the target node which can

support an agent and then begins tracing traffic". There is no mention that the device is upstream of a victim machine or of determining a set of routers that are neighbors of r.

The Examiner, citing col. 17, lines 32-51, for support, contends that Yavatkar discloses "for each neighbor n of r, determining if r is n's next-hop for traffic addressed to v, or to a network that v is on, where node n's next-hop for traffic addressed to v is the IP address of the node that n will forward a packet to if the destination address in the packet is v", as recited in claim 1. This contention is incorrect. The language in the cited text does not say anything about looking at a routing table on a neighbor to see if that neighbor will forward to r traffic that is addressed to v. This recited feature is advantageous as it can trace back to the source of a short-lived and bursty attack even if there is a temporary (or not so temporary) lull in the attack traffic from the source.

The Examiner, citing col. 17, lines 52-67, for support, contends that Yavatkar discloses the step of "after determining the identity of a neighbor ..." Yavatkar's system does not disclose or teach using next-hops to trace an attack back to a source as recited in claim 1.

With respect to claim 9, the Examiner, citing col. 13, lines 30-43, as support, contends that Yavatkar discloses the subject matter of claim 9. However this text merely describes uses of Yavatkar's system as noted in the above discussion of claim 1. The Examiner also refers to col. 17, lines 32-51, for further support, but this text does not include all of the concepts alleged by the Examiner. For example, contrary to the Examiner's assertion, the cited text does not include the concepts of "determining if r is n's next-hop for traffic addressed to v ..." and "further controlling operation of the data processor for the case where r is not n's next-hop for traffic addressed to v, to skip over n and query the next neighbor of r ...".

Claims 2 and 5 each depend on claim 1. Therefore, the rejection of claims 2 and 5 is erroneous for the same reasons set forth in the discussion of claim 1.

Claims 10 and 12 each depend on claim 9. Therefore, the rejection of claims 10 and 12 is erroneous for the same reasons set forth in the discussion of claim 9.

Further with respect to claims 2 and 10, the Examiner, citing col. 15, lines 42-62, as support, contends that Yavatkar discloses that the step of determining the set of neighbors comprises a step of sending at least one query to r to obtain information from a MIB that stores IP addresses of routers that are neighbors of r. However, the cited text says nothing about determining the set of neighbors, nothing about an MIB and nothing about a query etc. The cited text actually discusses about how a "watchdog agent" can act as a proxy and perform a "watchdog" function for another node, e.g., if the other node cannot perform the watchdog function.

Further with respect to claims 5 and 12, the Examiner, citing col. 15, lines 42-62, as support, contends that Yavatkar discloses that the step of determining an amount of traffic comprises a step of sending at least one message to a neighbor router n for determining a count of packets that router n is sending to router r that are addressed to v or to a network on which v resides. This contention is incorrect. Rather the cited text actually discusses about how a "watchdog agent" can act as a proxy as explained in the discussion of claims 2 and 10 above.

With respect to claim 16, the Examiner used the text of claim 1 to describe how claim 16 is met by Yavatkar. However, the texts of claims 1 and 16 have substantial differences. However, it is noted that Yavatkar lacks the determining and querying steps of claim 16 for the same reasons set forth in the discussion of claim 1.

Claims 17-19 and 21 each depend on claim 16. Therefore, the rejection of claims 17-19 and 21 is erroneous for the same reasons set forth in the discussion of claim 16.

Further with respect to claim 18, the Examiner, citing col. 16, lines 22-45, as support, contends that Yavatkar discloses "that the step of querying comprises....addressed to v". This contention is not correct. Claim 18 has to do with doing successive queries separated by some fixed amount of time to determine the packet rate. This is not discussed in the text cited by the Examiner.

Further with respect to claim 19, contrary to the Examiner's assertion, there is no language in the cited text that refers to "sending at least one message to a packet router for determining the number of packets to or towards v".

Further with respect to claim 21, the Examiner, citing col. 16, lines 50-65, as support, contends that Yavatkar discloses that the traceback function operates "on a plurality of selected paths, wherein a particular path is selected based at least on an amount of traffic flowing through the path". The Examiner's contention is untenable. The Examiner notes "that a particular path is selected". In contrast, claim 21 refers to tracing back along each of multiple paths.

For the reason set forth above, it is submitted that the rejection of claims 1, 2, 5, 9, 10, 12, 16-19 and 21 under 35 U.S.C. 102(b) as anticipated by Yavatkar is erroneous and should be withdrawn.

The Office Action rejects claims 3, 4 and 11 under 35 U.S.C 103(a) as unpatentable over Yavatkar as applied to claims 1 and 9 in view of U.S Patent No. 6,535,507 to Li et al., hereafter Li.

This rejection is untenable because Yavatkar lacks certain steps or elements recited in independent claims 1 and 9, upon which claims 3, 4 and 11 are dependent, as noted in the discussion of independent claims 1 and 9 above. Li does not supply these lacking steps or elements. Therefore, the rejection is untenable.

The Examiner admits that Yavatkar does not disclose the step of determining as recited in claim 3 or the step of sending as recited in claims 4 and 11, but contends that Li does, citing Li's col. 6, lines 46-54. This contention is untenable because the cited passage does not disclose either step or element. Although Li mentions next-hop resolution tables in an implementation for forwarding a message toward a destination node, there is no teaching of an implementation that determines if r is n's next-hop for traffic addressed to v, as recited in claim 3. Also, Li does not mention an IP forwarding table MIB or a query to a router regarding an entry in an IP forwarding table as recited in claims 4 and 11.

For the reasons set forth above, it is submitted that the rejection of claims 3, 4 and 11 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claims 6 and 13 under 35 U.S.C 103(a) as unpatentable over Yavatkar as applied to claims 1 and 9 in view of U.S Patent No. 5,963,540 to Bhaskaran, hereafter Bhaskaran.

This rejection is untenable because Yavatkar lacks certain steps or elements recited in independent claims 1 and 9, upon which claims 6 and 13 are dependent, as noted in the discussion of independent claims 1 and 9 above. Li does not supply these lacking steps or elements. Therefore, the rejection is untenable.

Furthermore, contrary to the Examiner's contention, the cited text at col. 1, lines 53-67, does not teach "establishing a black hole host route to v as close as possible to the source of attack", as recited in claims 6 and 13. The cited text just says that when a router is broken, packets may not be delivered and mentions that this is akin to sending them into a "black hole". The cited text does not teach the intentional introduction of a black hole close to a source of attack. This mitigates the effects of a denial of service attack.

For the reason set forth above, it is submitted that the rejection of claims 6 and 13 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claims 7 and 14 under 35 U.S.C 103(a) as unpatentable over Yavatkar as applied to claims 1 and 9 in view of U.S Patent No. 6,636,509 to Hughes, hereafter Hughes.

This rejection is untenable because Yavatkar lacks certain steps or elements recited in independent claims 1 and 9, upon which claims 7 and 14 are dependent, as noted in the discussion of independent claims 1 and 9 above. Hughes does not supply these lacking steps or elements. Therefore, the rejection is untenable.

Furthermore, the Examiner's argument is a little confusing because the Examiner has not specifically identified a specific teaching of Hughes or how the cited text is being read on the claim language. Applicant believes that the cited text is completely inapplicable to claims 7 and 14. Without this input, the Examiner has not made a prima facie case.

For the reasons set forth above, it is submitted that the rejection of claims 7 and 14 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claims 8 and 15 under 35 U.S.C 103(a) as unpatentable over Yavatkar as applied to claims 1 and 9 in view of U.S Patent No. 6,298,041 to Packer, hereafter Packer.

This rejection is untenable because Yavatkar lacks certain steps or elements recited in independent claims 1 and 9, upon which claims 8 and 15 are dependent, as noted in the discussion of independent claims 1 and 9 above. Packer does not supply these lacking steps or elements. Therefore, the rejection is untenable.

Furthermore, although Packer may teach rate limiting, Packer does not teach using rate limiting as a mechanism to deal with a denial-of-service attack. Also, Packer does not teach a step of establishing a rate limit for packets addressed to a victim machine as close as possible to the source of the denial-of-service attack packets as claimed in claims 8 and 15.

For the reasons set forth above, it is submitted that the rejection of claims 8 and 15 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claims 20 under 35 U.S.C 103(a) as unpatentable over Yavatkar as applied to claim 16 in view of U.S Patent No. 6,456,597 to Bare, hereafter Bare.

This rejection is untenable because Yavatkar lacks certain steps recited in independent claim 16, upon which claim 20 is dependent, as noted in the discussion of independent claim 16 above. Packer does not supply these lacking steps or elements. Therefore, the rejection is untenable.

Furthermore, Bare does not teach at col. 41, line 66 to col. 42 line 45, establishing a black hole host route to a victim of a denial of service attack, v, as

close as is possible to the source of the undesirable packets as contended by the Examiner. The cited text simply says that in the scenario described in Bare things can go wrong, a "routing loop" can occur resulting in packets getting lost in a "black hole".

Applicant believes the Examiner is also incorrect in asserting that Bare at col. 38, line 33 to col. 39, line 13, teaches "establishing a special host route to v using the same next hop as an existing route, the special host route tracking changes in the existing route such that when a next hop for the existing route changes, the next hop for the host route changes similarly." Applicant could not find in the cited text anything about routes to victims of an attack, or host routes to victims of an attack or a special host route to a victim that uses the same next hop as an existing route that carries traffic to that host or the use of a special route that tracks changes to an existing route etc.

Moreover, contrary to the Examiner's assertion, applicant does not believe the cited text in Bare teaches establishing a rate limit for packets addressed to a victim, v, as close as possible to the source of the denial-of-service attack. The cited reference makes no mention of a denial-of-service attack, a source of a denial of service attack, the concept of being close or as close as possible to a source of a denial of service attack or using rate limiting as a means for dealing with a denial-of-service attack.

For the reasons set forth above, it is submitted that the rejection of claim 20 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claim 22 under 35 U.S.C 103(a) as unpatentable over Yavatkar in view of U.S Patent No. 5,963,540 to Bhaskaran, hereafter Bhaskaran.

This rejection is untenable because the combination of Yavatkar and Bhaskaran lacks all the steps of claim 22. Yavatkar lacks all of the steps for the reasons noted above in the discussion of claim 1 and Bhaskaran lacks the step of establishing a black hole host route as recited for the reason noted above in the discussion of claims 6 and 13.

For the reason set forth above, it is submitted that the rejection of claim 22 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action cites a number of patents that were not applied in the rejections of the claims. These patents have been reviewed, but are believed to be inapplicable to the claims.

It is respectfully requested for the reasons set forth above that the rejections under 35 U.S.C. 102(b) and 35 U.S.C. 103(a) be withdrawn, that claims 1-23 be allowed and that this application be passed to issue.

Respectfully Submitted,

Date: 9/28/05

Paul D. Greeley
Reg. No. 31,019
Attorney for Applicant
Ohlandt, Greeley, Ruggiero & Perle, L.L.P.
One Landmark Square, 10th Floor
Stamford, CT 06901-2682
(203) 327-4500